

Implementasi *Fault Management* (Manajemen Kesalahan) Pada *Network Management System* (NMS) Berbasis SNMP

Yuli Sholikatin, Nur Rohman Rosyid

Teknologi Jaringan Departemen Teknik Elektro dan Informatika,

Universitas Gadjah Mada, Yogyakarta

yuli.sholikatin@mail.ugm.ac.id

Teknologi Jaringan Departemen Teknik Elektro dan Informatika,

Universitas Gadjah Mada, Yogyakarta

nrohmanr@ugm.ac.id

Abstract-- The use of computer network technology to meet the needs of information quickly and diverse, resulting in the increasingly widespread and increasing complexity of a computer network. Therefore, we need a supporting facility to be able to supervise the network element that is by using Network Management System (NMS). The NMS model established by ISO includes 5 conceptual areas, there are Fault, Configuration, Accounting, Performance and Security Management (FCAPS). One area that will be implemented in this research is Fault Management. The mechanism that will be used for error management is by detecting the occurrence of errors and sending notifications via email when the error appears, then logging report and make a diagnosis and to further recommend the solution to the error. The type of error reported in this system is errors when there is a failure of connectivity on the network device, errors due to services that are not running and not in accordance with the request, errors when high RAM usage, CPU load increases and the use of hard drives which started full. From the research results obtained, built NMS can send error notification and give solution recommendation via email to the network admin so if there is a network error, Fault Management activities can be done as early as possible so that the problem does not result in the deterioration of network quality.

Kata kunci--Network Management; NMS; Fault Management; SNMP; System Information

I. PENDAHULUAN

Penggunaan teknologi jaringan komputer untuk memenuhi kebutuhan informasi yang cepat dan beragam dari waktu ke waktu semakin meningkat. Oleh karena itu, manajemen jaringan menjadi satu hal yang perlu diperhatikan, apabila jaringan komputer tersebut sudah semakin luas dan bertambah kompleks. Tiga hal penting

yang harus diperhatikan dalam mengelola jaringan yang kompleks diantaranya struktur, manajemen dan efektivitas dari jaringan tersebut [10].

Masalah-masalah jaringan yang sering ditemui di lapangan diantaranya kerusakan elemen jaringan seperti *hub*, *bridge*, *router*, *server*, bahkan sampai ke *transmission facilities* [11]. Kesalahan jaringan tersebut seringkali tidak dapat diketahui oleh seorang admin jaringan dan penanganan masalah menjadi terlalu lama sehingga berakibat fatal pada penurunan kualitas jaringan.

Untuk mengatasi kesalahan jaringan tersebut diperlukan suatu fasilitas pendukung untuk dapat melakukan pengawasan terhadap elemen jaringan yakni dengan menggunakan *Network Management System* (NMS). *Network Management* atau manajemen jaringan merupakan kemampuan untuk memonitor, mengontrol, dan merencanakan suatu jaringan komputer dan komponen sistem. Penggunaan NMS ini akan sangat membantu admin jaringan dalam mengelola dan memelihara infrastruktur jaringan dengan topologi yang kompleks.

Model NMS yang ditetapkan ISO mencakup 5 area konseptual yaitu *Fault*, *Configuration*, *Accounting*, *Performance* dan *Security Management* (FCAPS) [8]. Salah satu area yang akan diimplementasikan pada penelitian kali ini adalah *Fault Management* (Manajemen Kesalahan). Adapun fungsi *Fault Management* ini adalah untuk mendeteksi, mencatat, memberitahu pengguna, dan memperbaiki kesalahan jika memungkinkan. Dengan memanfaatkan *Fault Management* akan memungkinkan administrator jaringan untuk mengetahui kesalahan (*fault*) pada perangkat yang

dikelola agar dapat segera menentukan apa penyebabnya dan dapat segera mengambil tindakan perbaikan.

Network Management System (NMS) merupakan implementasi dari model FCAPS dimana standar yang digunakan yaitu *Simple Network Management Protocol* (SNMP). SNMP merupakan sebuah protokol yang didesain untuk memberikan kemampuan kepada pemakai guna mengelola jaringan komputernya dari jarak jauh atau remote. Data yang didapatkan dari SNMP ini tidak hanya berupa status up/down, juga berupa informasi penting lainnya seperti utilisasi dari cpu (*cpu utilization*), memori (*memory utilization*), tipe perangkat, trafik yang terbaca untuk setiap port, sampai versi sistem operasi yang digunakan.

Perancangan dan implementasi sebuah aplikasi NMS merupakan solusi yang efektif dalam mencari dan menemukan kesalahan (*fault*) yang terdapat pada suatu jaringan, sehingga dapat dilakukan penanganan sedini mungkin agar masalah tersebut tidak berakibat pada penurunan kualitas jaringan.

II. TINJAUAN PUSTAKA

Penelitian oleh Farisa Lutfi Amar [1] memanfaatkan Nagios Icinga sebagai aplikasi kolektor informasi server untuk memantau status dan kondisi perangkat jaringan serta mengirimkan notifikasi kepada admin jaringan ketika terjadi gangguan pada perangkat melalui email dan twitter.

Sementara itu, Defrid Onisimus Benu dan Dian W. Chandra [2] memodifikasi aplikasi OpenNMS untuk mengetahui kesalahan-kesalahan dan gangguan-gangguan yang terjadi dalam jaringan WDS serta memonitoring status dari *access point*, dan mengirimkan

notifikasi perangkat yang *down* kepada administrator melalui email.

Dalam literatur lain oleh Mohammad Solehfuiddin dkk [12] merancang sebuah aplikasi *smartphone android* untuk memantau jaringan LAN secara *remote* (dari jarak jauh) serta memberitahukan informasi kesalahan dengan mengaktifkan notifikasi di Android dan membuat metode penanganan kesalahan pada server secara remote. Aplikasi ini dapat dijalankan pada perangkat Android dengan versi sistem operasi minimum KitKat (4.4) maupun versi terbaru pada sistem operasi Android.

Peneliti lain Asep Fauzi Mustaqin [7] melakukan monitoring keamanan jaringan secara real time menggunakan SNORT kemudian mengirimkan notifikasi melalui SMS saat mendeteksi adanya intrusi jaringan (penyusupan, penyerangan, pemindaian dll). Sistem ini juga memanfaatkan teknologi BASE sebagai *interface web* untuk melakukan analisis dari intrusi yang terdeteksi oleh SNORT dan melakukan pengujian sistem dengan menggunakan *PING attack*, *DOS/DDOS attack* serta *port scanning*.

Berdasarkan analisis tinjauan pustaka di atas, perbedaan penelitian yang sudah ada dengan penelitian yang akan dimulai saat ini, terangkum pada tabel perbandingan penelitian pada tabel I berikut. Penulis akan merancang dan membangun sistem mulai dari awal tanpa menggunakan aplikasi NMS yang sudah ada sebelumnya. Adapun sistem yang akan dibangun yakni berbasis web dengan Codeigniter sebagai framework PHP dan MySQL sebagai database server. Untuk sistem peringatan kesalahan (*error*) pada jaringan, penulis akan memanfaatkan email sebagai media penyampaian pesan kesalahan jaringan kepada administrator jaringan.

TABEL I.

PERBANDINGAN PENELITIAN

Peneliti	Judul	Tujuan	Sistem Peringatan	Metode	Informasi Kesalahan Yang diperingatkan
Farisa Lutfi Amar (2015) [1]	Sistem Pemantauan Perangkat Jaringan Berbasis Web dengan Notifikasi Email dan Twitter	<ul style="list-style-type: none"> Memantau status dan kondisi perangkat jaringan Mengirimkan notifikasi kepada admin jaringan ketika terjadi gangguan pada perangkat 	Email dan twitter	<ul style="list-style-type: none"> Nagios Icinga sebagai aplikasi kolektor informasi server Perancangan aplikasi web sebagai aplikasi pendukung Nagios Perancangan API sebagai penghubung antara Nagios dengan Twitter Server hanya bersifat simulasi dengan menggunakan mesin virtual 	<ul style="list-style-type: none"> Penggunaan RAM yang tinggi Load CPU yang meningkat cepat Media penyimpanan harddisk yang mulai penuh Adanya layanan yang tidak berjalan
Defrid Onisimus Benu dan Dian W. Chandra	Penerapan <i>Fault Management</i> Menggunakan <i>Open Network Management</i>	<ul style="list-style-type: none"> Mendeteksi dan menampilkan kesalahan pada perangkat access point di jaringan WDS Mengirimkan notifikasi 	Email	<ul style="list-style-type: none"> Melakukan modifikasi aplikasi OpenNMS Membangun jaringan WDS dengan tiga <i>access point</i> yang akan dimonitoring 	Status <i>error/DOWN</i> pada <i>access point</i>

(2016) [2]	<i>System (OPENNMS)</i> Pada	kepada administrator jaringan ketika terdapat perangkat yang down			
Muhammad Solehuddin, Sugiyono, Muryan Awaludin (2016) [12]	Penerapan Simple Network Management Protocol Pada FCAPS untuk Monitoring Server Berbasis Android Studi Kasus PT. JARING SYNERGI MANDIRI	<ul style="list-style-type: none"> • Memantau LAN secara remote (dari jarak jauh) melalui smartphone (Android) • Memberitahukan informasi kesalahan dengan mengaktifkan notifikasi di Android • Metode penanganan kesalahan pada server secara remote melalui Android 	Aplikasi smartphone (Android)	<ul style="list-style-type: none"> • Pada sisi front-end, menggunakan bahasa pemrograman JAVA dengan editor Android Studio • Pada sisi back-end menggunakan bahasa PHP dengan framework CI • Database MySQL • Dalam pertukaran data antara web server dengan perangkat Android, menggunakan JASON sebagai media interface 	Semua <i>error</i> terkait server dan jaringan yang dimonitoring
Asep Fauzi Mutaqin (2016) [7]	Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort	<ul style="list-style-type: none"> • Memonitoring keamanan jaringan secara real time menggunakan snort • Mengirimkan notifikasi melalui SMS saat mendeteksi adanya intrusi jaringan (penyusupan, penyerangan, pemindaian dll) 	SMS	<ul style="list-style-type: none"> • Menggunakan SNORT untuk mendeteksi sebuah serangan atau penyusup dalam jaringan • BASE sebagai interface web untuk melakukan analisis dari intrusi yang terdeteksi oleh snort • Pengujian menggunakan PING attack, DOS/DDOS attack dan port scanning 	Semua serangan yang masuk pada jaringan. Seluruh paket yang masuk kedalam jaringan akan dibandingkan oleh detection engine apakah sesuai dengan rules atau tidak.
Yuli Sholikatin (2017)	Rancang Bangun Aplikasi <i>Network Management System</i> (NMS) Untuk <i>Fault Management</i> (Manajemen Kesalahan) Berbasis SNMP	<ul style="list-style-type: none"> • Mendeteksi terjadinya kesalahan • Melaporkan kesalahan yang muncul melalui email • Mencatat laporan kesalahan (logging) • Melakukan diagnosis dan memberikan rekomendasi solusi 	Email	<ul style="list-style-type: none"> • Membangun aplikasi berbasis web • Codeigniter sebagai framework PHP • MySQL sebagai server basisdata • Membangun server sungguhan dengan Ubuntu Server 16.04 LTS (bukan virtual) 	<ul style="list-style-type: none"> • Konektivitas antar perangkat jaringan • Adanya layanan yang tidak berjalan dan tidak sesuai dengan <i>request</i> • Penggunaan RAM yang tinggi • <i>Load</i> CPU meningkat cepat • Hardisk yang mulai penuh

III. LANDASAN TEORI

A. Manajemen Jaringan

Manajemen jaringan adalah sebuah aktivitas, metode, prosedur dan peralatan yang berhubungan dengan proses operasi, administrasi, pemeliharaan dan penyediaan dari sebuah sistem jaringan. [3]

Aplikasi Manajemen Jaringan atau biasa disebut *Network Management System* (NMS) merupakan aplikasi web yang terintegrasi dengan aplikasi desktop. NMS dikenal juga dengan sistem monitoring jaringan menggambarkan sebuah sistem yang terus menerus memonitor jaringan komputer sehingga jika terjadi gangguan dalam jaringan dapat secepatnya memberikan notifikasi kepada administrator jaringan.

Model NMS yang ditetapkan ISO mencakup 5 area konseptual yaitu *Fault Management*, *Configuration Management*, *Accounting Management*, *Performance Management* dan *Security Management* (FCAPS).

B. Fault Management

Fault Management adalah mendeteksi, mengisolasi dan memperbaiki operasi – operasi yang tidak normal dalam jaringan. *Fault Management* meliputi lima langkah proses yaitu : pendeteksian masalah, mencari tempat permasalahan, merestorasi layanan, mengidentifikasi akar penyebab permasalahan dan resolusi pemecahan masalah. *Fault Management* melibatkan 5 tahap proses : *Fault detection*, *fault location*, *service restoration*, *identification*, dan *problem resolution*.

C. SNMP

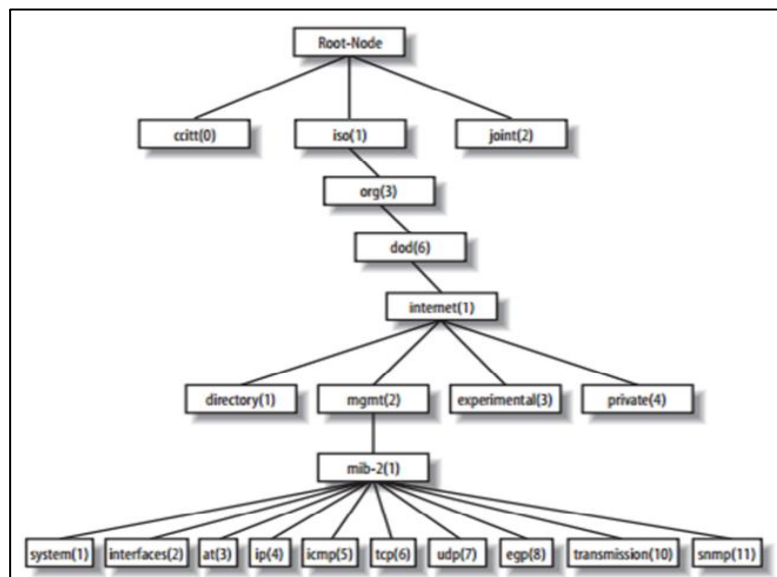
Simple Network Management Protocol (SNMP) merupakan sebuah protokol yang didesain untuk memberikan kemampuan kepada pemakai untuk mengelola jaringan komputernya dari jarak jauh atau remote. Pengelolaan ini dilaksanakan dengan cara melakukan polling dan setting variabelvariabel elemen jaringan yang dikelolanya [5].

Ada 3 elemen yang memegang peranan penting saat kita mempelajari SNMP, yaitu :

1. **Manajer.** Sebuah manager merupakan sebuah server yang menjalankan beberapa macam perangkat lunak yang berfungsi melakukan pengelolaan jaringan. Manager bertanggung jawab dalam berkomunikasi dengan *agent* pada perangkat jaringan yang dimonitor untuk mendapatkan informasi [4].
2. **Agent.** *Agent* adalah perangkat lunak yang berjalan pada perangkat jaringan yang di-manage. *Agent* dapat berupa perangkat lunak terpisah (daemon), atau yang tergabung di dalam sistem operasi (CISCO IOS pada CISCO Router) [14].
3. **MIB.** MIB (*Management Information Database*) merupakan tempat penyimpanan informasi yang dimiliki oleh agen yang nantinya diakses oleh *Network Management System* (NMS). Informasi yang disimpan oleh MIB menggunakan diagram pohon dan menempatkan *Object Identifier* (OID) pada setiap node pohon. Diagram pohon MIB tergambarkan pada Gambar 1 di bawah ini. OID berupa integer yang dipisahkan oleh dots (.). Objek – objek informasi SNMP memperoleh kedudukan di bawah node mib-2(1). Untuk mengakses objek – objek tersebut maka harus dituliskan sesuai urutan node seperti yang dijelaskan pada tabel II di bawah ini.

TABEL II. MIB-II GROUPS

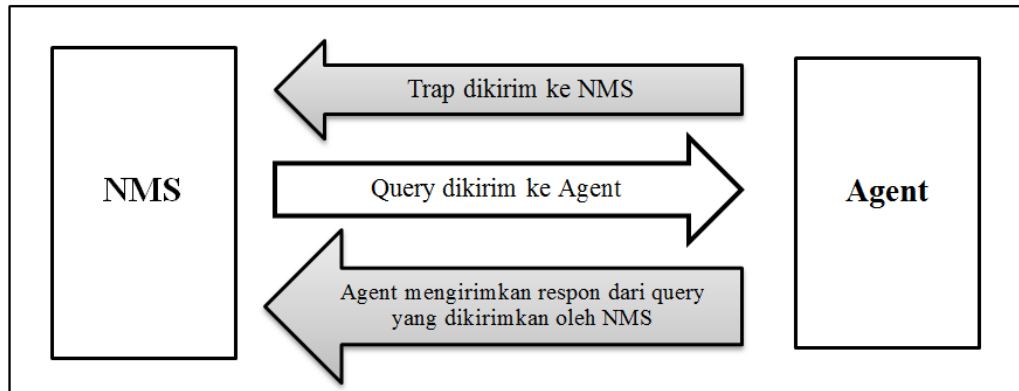
Subtree name	OID	Deskripsi
sistem	1.3.6.1.2.1.1	Mendefinisikan objek yang berhubungan dengan sistem operasi, uptime, system contact, dan system name
interface	1.3.6.1.2.1.2	Melacak status interface perangkat
at	1.3.6.1.2.1.3	Alamat terjemahan
ip	1.3.6.1.2.1.4	Melacak beberapa aspek dari IP, termasuk IP Routing
icmp	1.3.6.1.2.1.5	Melacak ICMP <i>error</i>
tcp	1.3.6.1.2.1.6	Melacak koneksi TCP
udp	1.3.6.1.2.1.7	Melacak statistik UDP
egp	1.3.6.1.2.1.8	Melacak statistik dari Exterior Gateway Protocol (EGP) dan menyimpannya dalam EGP tabel
transmission	1.3.6.1.2.1.9	Tidak ada objek yang didefinisikan pada grub ini, tetapi ada beberapa perangkat mendefinisikan pada objek ini
snmp	1.3.6.1.2.1.10	Mengukur kinerja SNMP seperti melacak paket yang dikirim dan diterima



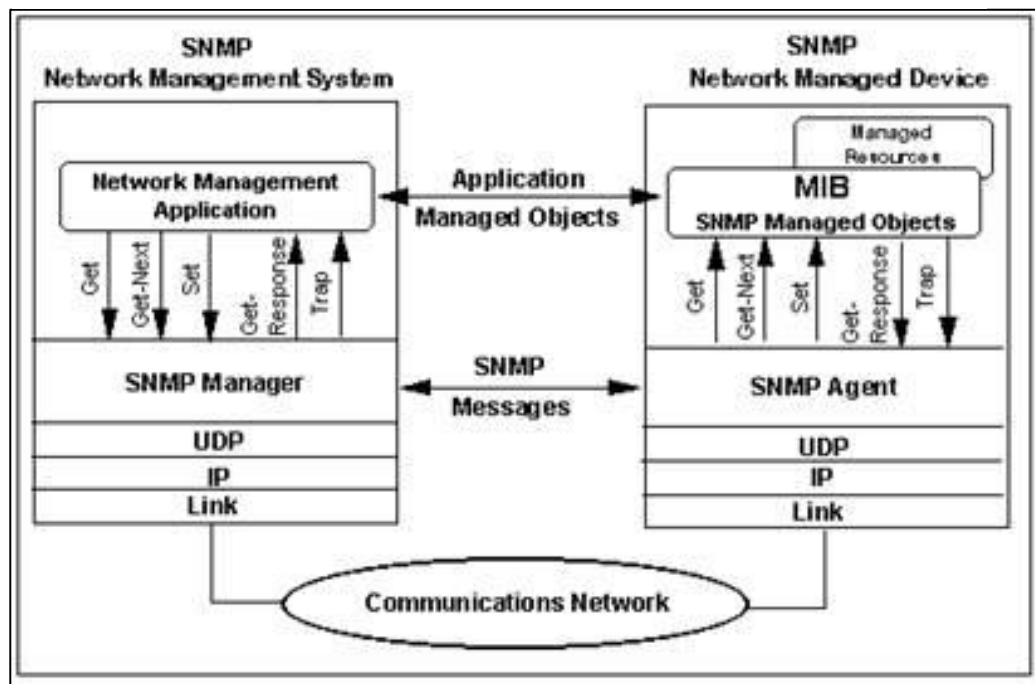
Gambar 1. MIB Tree

Protokol SNMP menggunakan konsep NMS (*Network Management System*) dan *agent*. NMS berperan untuk melakukan *polling* dan menerima *trap* dari *agent*. *Poll* adalah aksi melakukan *query* pada *agent* (router, komputer, dan lain-lain) yang dapat digunakan jika terjadi suatu masalah pada perangkat tersebut. *Trap* ialah cara *agent* dalam memberitahu NMS bila terjadi sesuatu yang abnormal. Adapun

gambaran interaksi pesan *trap* antara NMS dan *agent* telah tergambarkan pada gambar 2 berikut. Sedangkan untuk prinsip kerja SNMP dapat dilihat ilustasinya pada gambar 3 di bawah ini.



Gambar 2. Interaksi Pesan Trap antara NMS dan *Agent*



Gambar 3. Prinsip Kerja SNMP

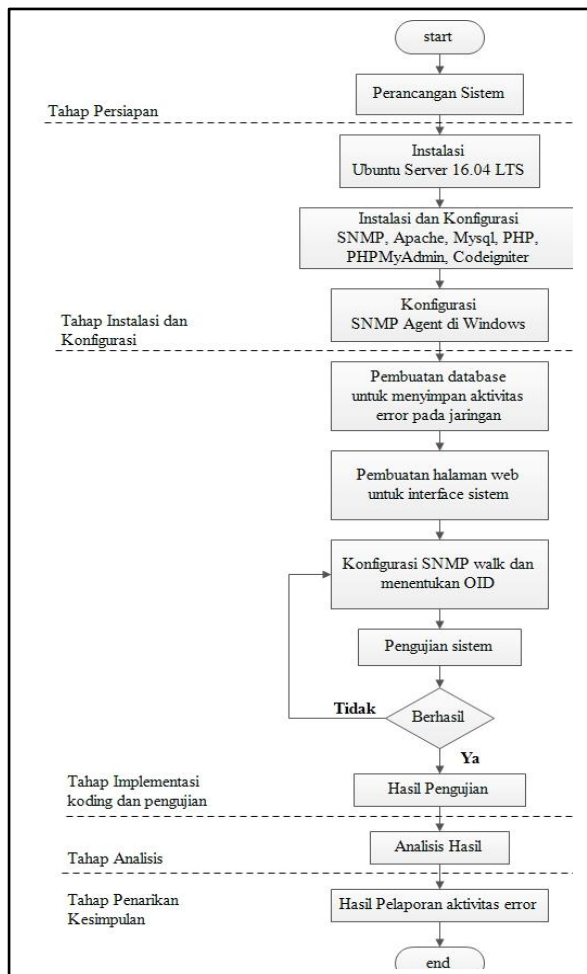
IV. HASIL DAN PEMBAHASAN

A. Tahapan Proses

Dalam pengerjaan penelitian ini, tahapan-tahapan yang dilakukan, yaitu perancangan topologi jaringan yang nanti akan diimplementasikan, perancangan

database dan perancangan *User Interface*, kemudian melakukan instalasi dan konfigurasi semua perlengkapan yang dibutuhkan, implementasi koding sekaligus pengujian, dan yang terakhir melakukan analisis hasil yang diperoleh untuk mendapatkan suatu kesimpulan.

Tahapan proses penelitian tergambarkan dengan *flowchart* pada gambar 4 berikut.

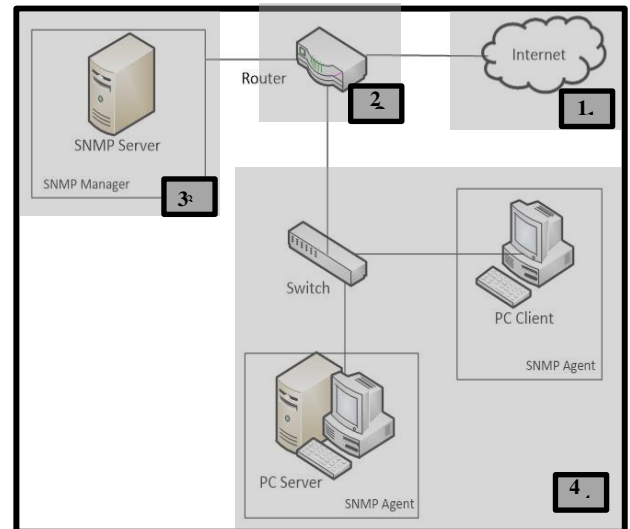


Gambar 4. Tahapan Proses Penelitian

- **Tahap Persiapan** : merupakan tahap membuat sebuah rancangan sistem yang diperlukan dalam pembuatan aplikasi untuk manajemen kesalahan jaringan diantaranya pembuatan rancangan topologi jaringan, database dan *User Interface* sistem.
- **Tahap Instalasi dan Konfigurasi** : merupakan tahap menginstal dan mengkonfigurasi semua perlengkapan yang dibutuhkan seperti Ubuntu server dan service-service yang berjalan di dalamnya, serta mengkonfigurasi *SNMP agent*.
- **Tahap Implementasi dan Pengujian** : merupakan tahap menerapkan hasil rancangan dengan koding dan selanjutnya menguji proses-proses pada sistem yang sudah dibangun agar sesuai dengan kebutuhan dan mencari kesalahan/kekurangan dari sistem untuk meminimalisir cacat program (*bug*).

- **Tahap Analisis** : merupakan tahapan mengolah hasil pengujian untuk selanjutnya dapat ditarik suatu kesimpulan.

Adapun perancangan topologi yang digunakan pada penelitian ini tergambar pada gambar 5 di bawah ini.



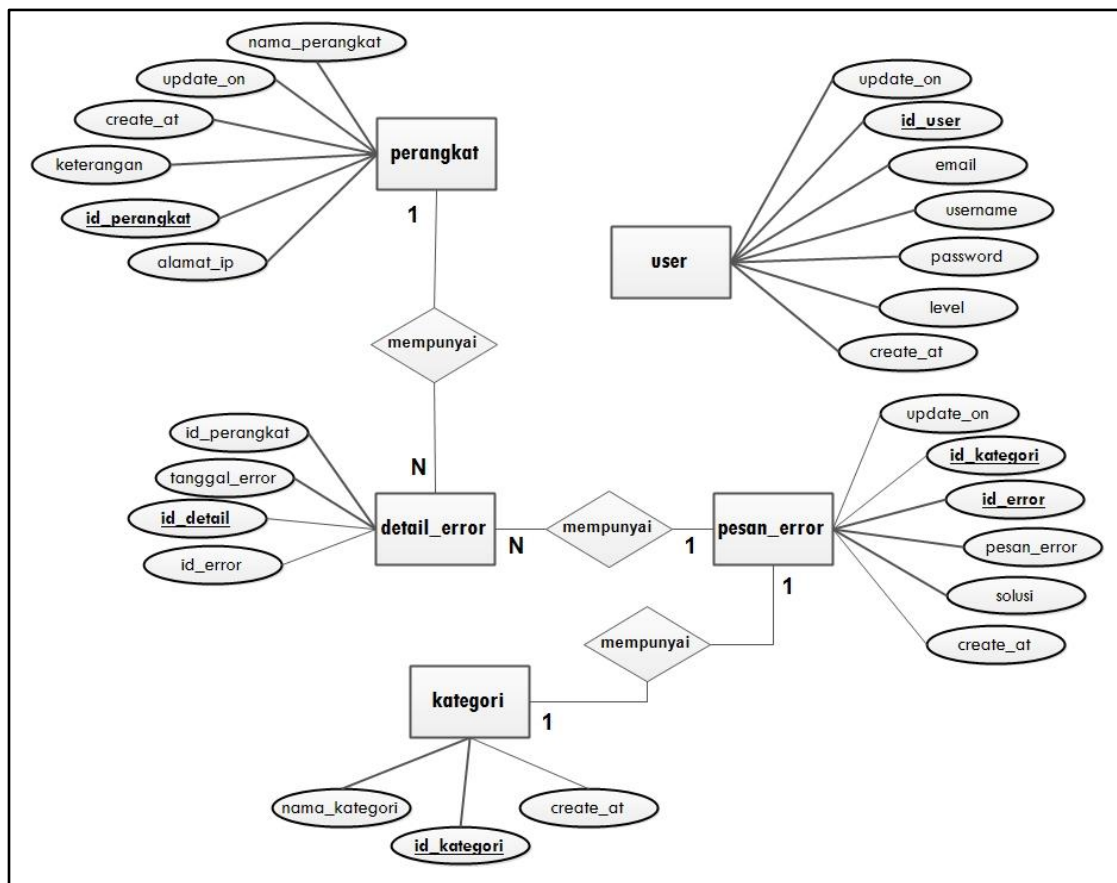
Gambar 5. Perancangan Topologi Jaringan

Keterangan :

1. Sumber Internet
2. Router
3. Sebuah PC yang akan diinstal Ubuntu Server 16.04 LTS untuk diaktifkan sebagai *SNMP server*. Pada PC server tersebut juga dilakukan instalasi dan konfigurasi service-service yang berjalan, yakni : *SNMP*, *Apache* sebagai *web server*, *MySQL* sebagai *database server*, *PHP* sebagai *server side scripting*, *PhpMyAdmin* sebagai *software database*, dan *Codeigniter* sebagai *framework PHP*.
4. Jaringan yang akan dimonitoring yang nanti akan diambil *log activity*-nya, dimana masing-masing perangkat jaringan tersebut akan diaktifkan sebagai *SNMP Agent*.

B. Perancangan Sistem Manajemen Kesalahan Jaringan

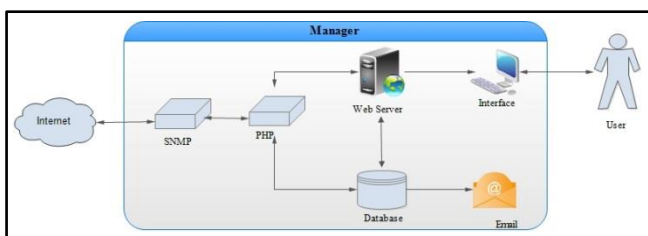
Database digunakan sebagai media penyimpanan data aktivitas kesalahan (*error*) jaringan yang kemudian digunakan untuk menghasilkan informasi berupa pelaporan aktivitas *error* jaringan. Dalam sistem ini, perancangan basis data dibuat berdasarkan *Entity Relationship Diagram* (ERD) yang nantinya dapat digunakan dalam pembuatan tabel-tabel basis data. Perancangan database sistem dapat dilihat pada gambar 6 berikut.



Gambar 6. Perancangan Basis Data

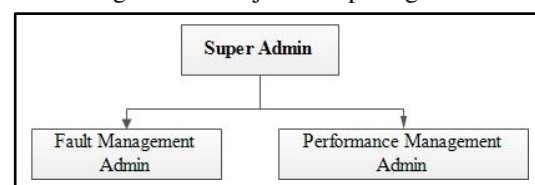
C. Gambaran Umum Sistem

Dalam penelitian ini akan dihasilkan sebuah sistem manajemen jaringan berbasis web atau biasa disebut *Network Managemen System* (NMS) dimana fokus utamanya adalah melakukan manajemen kesalahan pada jaringan. Atau pada penelitian ini kita sebut sebagai *Network Fault Management System*. Jadi, kejadian kesalahan (*error*) pada jaringan tersebut akan disimpan pada sebuah database khusus, untuk selanjutnya akan ditampilkan di sistem dan dikirimkan melalui email kepada admin jaringan. Arsitektur sistem manajemen ini ditunjukkan pada Gambar 7 berikut.



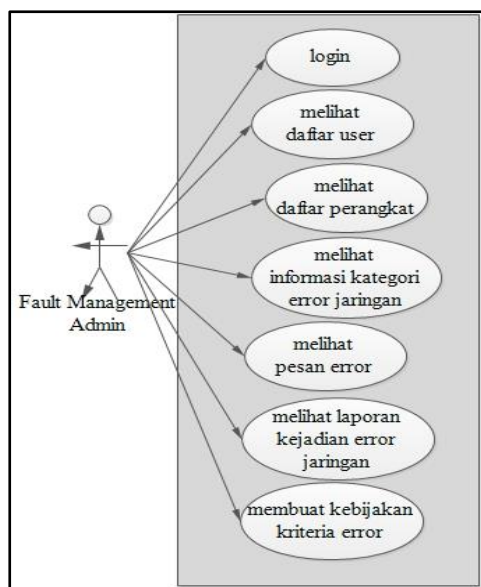
Gambar 7. Arsitektur Sistem

Penelitian ini merupakan *project* gabungan antara penulis dengan rekan penulis dimana terdapat 2 fungsi manajemen jaringan di dalamnya, yaitu fungsi *Fault Management* (oleh penulis sendiri) dan fungsi *Performance Management* (oleh rekan penulis). Sehingga user pada sistem ini ada 3, yakni : super admin, *Fault Management admin* dan *performance management admin*. Pada penelitian ini penulis hanya akan fokus pada user *Fault Management admin*. Sedangkan super admin adalah admin yang mempunyai wewenang tertinggi untuk menentukan hak akses user. Adapun gambaran mengenai struktur user dan relasi user *Fault Management Admin* dengan sistem dijelaskan pada gambar 8 berikut.



Gambar 8. Struktur User

Kebutuhan fungsional user *Fault Management Admin* dapat diilustrasikan pada gambar 9 *usecase* diagram di bawah ini.



Gambar 9. Usecase Diagram Fault Management Admin

Adapun kategori kesalahan (*error*) yang dilaporkan pada sistem ini ada 5 kategori *error*. Kesalahan (*error*) jaringan yang dimaksud adalah kesalahan ketika terjadi kegagalan konektivitas pada perangkat jaringan, kesalahan karena adanya layanan (*service*) yang tidak berjalan dan tidak sesuai dengan *request*, *error* ketika penggunaan RAM mulai tinggi, *load* CPU meningkat dan penggunaan hardisk yang mulai penuh. Untuk kriteria *error* pada masing-masing kategori dapat dilihat pada tabel III berikut.

TABEL III. KRITERIA ERROR

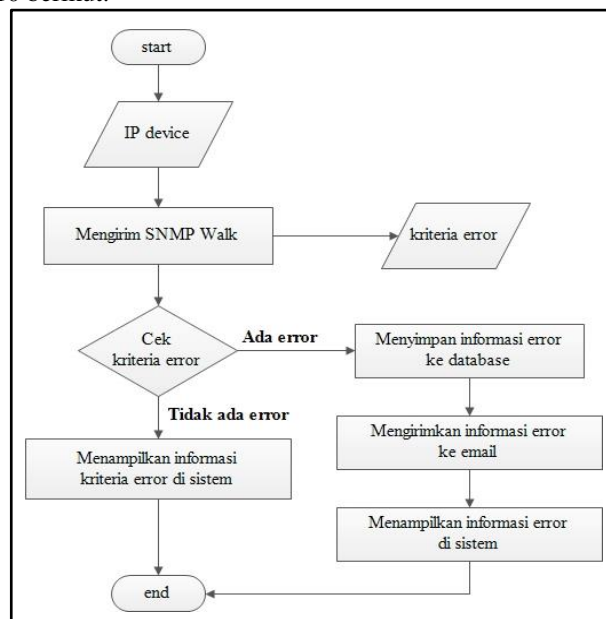
No	Kategori Error	Kriteria Error
1	Konektivitas	respon time > 450ms
2	Layanan	ketika layanan tidak berjalan
3	RAM Usage	> 85%
4	Load CPU	> 85%
5	Hardisk usage	> 85%

D. Proses Pendeteksian Error Otomatis

Sistem yang dihasilkan pada penelitian ini menggunakan protokol yang disebut dengan Simple Network Management Protocol (SNMP). SNMP bekerja dengan meminta nilai-nilai tertentu dari *agent* yang dimonitor dan *agent* akan menjawabnya berdasarkan OID yang diminta [9].

Proses pendeteksian kesalahan (*error*) otomatis pada sistem ini bekerja dengan mengirimkan sebuah konfigurasi SNMP walk berdasarkan OID tertentu untuk mendapatkan informasi kategori kesalahan dari *agent*. Setelah *agent* memberikan informasi berdasarkan OID yang dikirimkan, maka selanjutnya informasi tersebut akan dicek apakah memenuhi kriteria kesalahan yang diminta atau tidak. Jika memenuhi kriteria, maka informasi tersebut akan dianggap sebagai kejadian *error*

dan disimpan ke dalam database untuk selanjutnya kejadian *error* tersebut akan ditampilkan pada sistem dan dikirimkan melalui email [6]. Proses pendeteksian *error* otomatis ini tergambarkan pada *flowchart* pada gambar 10 berikut.



Gambar 10. Diagram Proses Pendeteksian Error Otomatis

E. Pengujian Sistem

Pada saat pertama kali menjalankan sistem, user akan dihadapkan pada sebuah halaman login. Halaman login ini merupakan halaman pembatas hak akses setiap pengguna dalam menggunakan setiap fitur pada sistem manajemen jaringan ini. Setelah proses login berhasil, selanjutnya seorang *Fault Management admin* akan diarahkan pada halaman beranda *Network Fault Management System*.

Pada tampilan halaman beranda sistem pada gambar 11, user akan mendapatkan beberapa informasi terkait kondisi terkini dari jaringan yang sedang dimonitoring. Adapun informasi yang ditampilkan pada sistem ini, yakni jumlah total pesan *error* yang masuk ke sistem, jumlah perangkat dalam kondisi UP/DOWN, jumlah layanan UP/DOWN, top 3 penggunaan RAM *Usage* tertinggi, top 3 *Load* CPU tertinggi dan top 3 Hardisk *Usage* tertinggi. Informasi ini bersifat realtime dan akan mengalami refresh setiap 1 menit sekali.

Selanjutnya, user juga dapat melihat data perangkat dan data user beserta level masing-masing user. Data perangkat ini berisi informasi detail mengenai perangkat-perangkat jaringan yang dimonitoring dan sebelumnya sudah terkonfigurasi sebagai *agent*.

User juga diberikan menu khusus dengan nama *Kriteria Error* untuk mendapatkan informasi serta status mengenai kategori *error* pada masing-masing perangkat. Menu *Kriteria Error* ini memiliki 5 submenu sesuai dengan nama kategori *error* yang dimonitoring pada

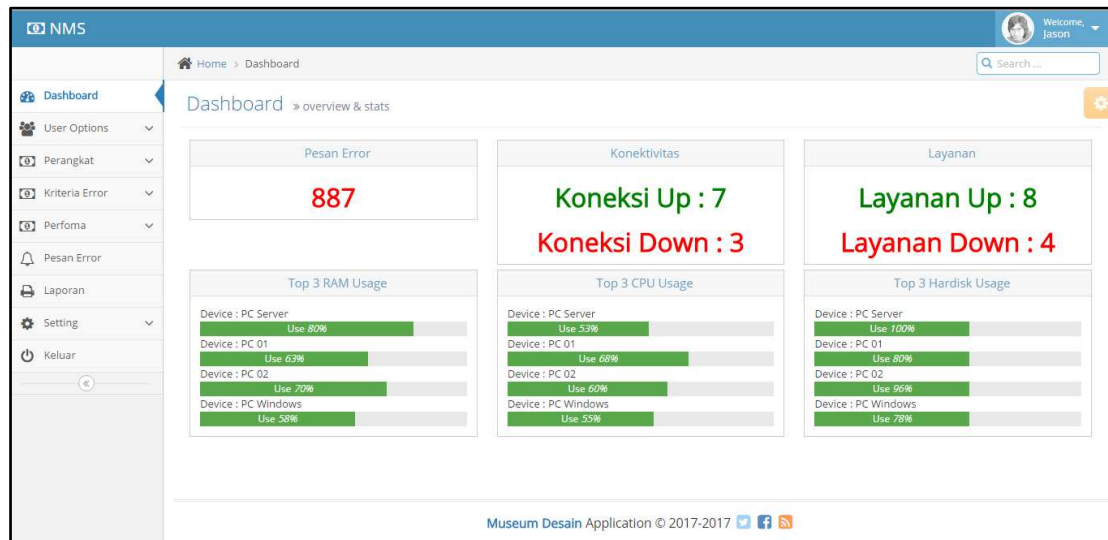
sistem ini, yakni sub menu Konektivitas, Data Layanan, RAM Usage, Load CPU dan Hardisk Usage.

Seluruh informasi pada masing-masing sub menu di menu Kriteria Error apabila berstatus *ERROR* maka akan dianggap sebagai kejadian *error* dan tertampilkan pada menu Pesan Error. Dapat dilihat pada gambar 12, Menu Pesan Error ini ditampilkan berdasarkan urutan waktu kejadian *error*. Pada menu ini user juga dapat memilih menampilkan pesan *error* sesuai kategori *error* pada menu *filtering* yang disediakan pada sistem. Adapun informasi kejadian *error* yang ditampilkan pada menu ini adalah waktu kejadian *error*, informasi *error*, kategori *error*nya, lokasi terjadinya *error* serta solusi penanganan *error*nya seperti apa.

Kejadian *error* yang terjadi selanjutnya akan disimpan ke dalam sebuah database khusus. Data-data tersebut selanjutnya akan diolah ke dalam sebuah menu Sebagaimana tergambarakan pada gambar 14, Menu Laporan yang berisi *report* kejadian *error* pada periode

waktu tertentu sesuai dengan waktu yang diinputkan user. Laporan ini berisi informasi mengenai total kejadian *error* pada tiap-tiap kategori *error* di masing-masing perangkat jaringan yang dimonitoring. Menu Laporan ini nantinya dapat digunakan untuk mengetahui komponen network mana yang rapuh/rentan *error* dan membutuhkan perhatian khusus dari *network administrator*.

Selain tertampilkan pada sistem, suatu kejadian *error* beserta rekomendasi solusi penanganan *error*-nya juga akan dikirimkan melalui email ke alamat email user/*Fault Management admin*. Adapun tampilan pesan *error* yang dikirimkan melalui email dapat dilihat pada gambar 13. Dengan adanya pengiriman notifikasi melalui email inilah diharapkan sebuah kejadian *error* jaringan dapat diketahui sedini mungkin oleh seorang admin jaringan, sehingga penanganan masalah tidak terlalu lama serta tidak berakibat fatal pada penurunan kualitas jaringan [13].

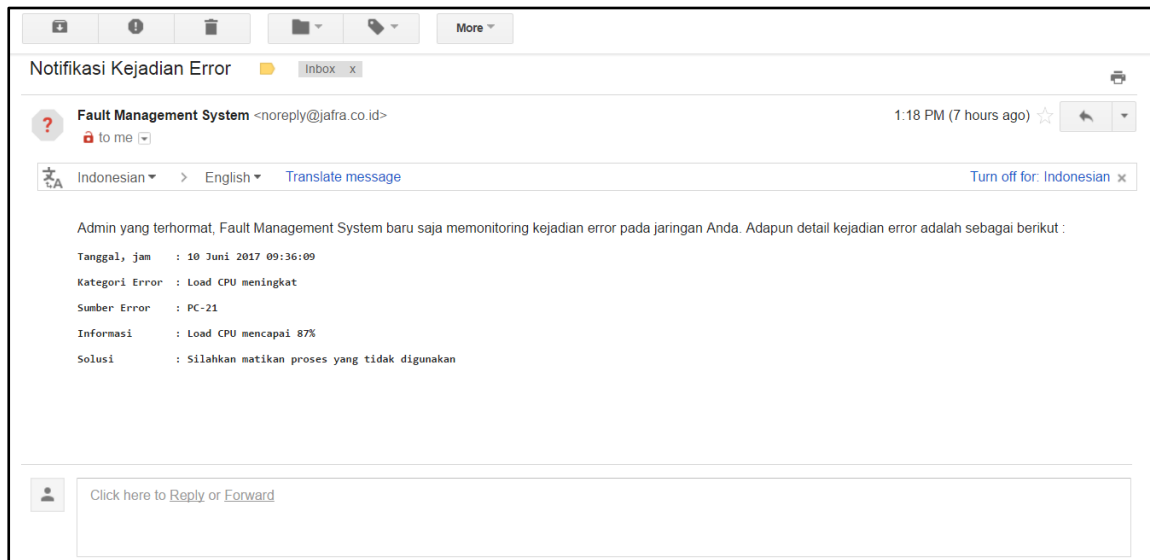


Gambar 11. Tampilan Beranda Sistem

The screenshot shows the 'Pesan Error' menu with a search bar and a table of error entries. The table has columns for No, Tanggal, Pesan, Kategori, Lokasi, Solusi, and Action. The entries list various errors such as 'Device is down', 'Package Loss is 87%', 'Memory Usage is 80%', 'SQL server is down', 'Package Loss is 81%', 'Package Loss is 83%', 'HTTP server is down', 'Hardisk Usage is 97%', 'Hardisk Usage is 88%', and 'Hardisk Usage is 88%'.

No	Tanggal	Pesan	Kategori	Lokasi	Solusi	Action
1	2017-11-19 18:47:55	Device is down	Konektivitas	PC Windows	Cek Koneksi ke device	
2	2017-11-19 13:13:14	Package Loss is 87%	Konektivitas	PC 01	Cek Koneksi Antar perangkat	
3	2017-11-17 16:31:45	Memory Usage is 80%	RAM Usage	PC 01	Silakan Matikan Proses yang tidak di gunakan	
4	2017-11-05 15:37:20	SQL server is down	Service	PC Windows	Hidupkan SQL server	
5	2017-10-21 12:32:35	Package Loss is 81%	Konektivitas	PC Server	Cek Koneksi Antar perangkat	
6	2017-10-15 04:22:48	Package Loss is 83%	Konektivitas	PC Server	Cek Koneksi Antar perangkat	
7	2017-09-30 17:00:25	HTTP server is down	Service	PC 01	Hidupkan service httpd	
8	2017-09-13 03:19:37	Hardisk Usage is 97%	Hardisk Usage	PC Windows	Hapus data yang tidak di perlukan	
9	2017-09-11 05:06:02	Hardisk Usage is 88%	Hardisk Usage	PC Server	Hapus data yang tidak di perlukan	
10	2017-09-01 18:58:21	Hardisk Usage is 88%	Hardisk Usage	PC Windows	Hapus data yang tidak di perlukan	

Gambar 12. Tampilan Menu Pesan Error Sistem



Gambar 13. Tampilan Pesan Error melalui Email

Laporan Kesalahan Jaringan							Beranda > Laporan
Dari tanggal			s/d		Cetak		
#	Nama Perangkat	Error Konektivitas	Error Layanan	Error RAM Usage	Error Load CPU	Error Hardisk Usage	Total
1	Komputer-1	10	XX	XX	XX	XX	XX
2	Komputer-2	5	XX	XX	XX	XX	XX
3	Komputer-3	6	XX	XX	XX	XX	XX
4	Komputer-4	7	XX	XX	XX	XX	XX
5	Komputer-5	0	XX	XX	XX	XX	XX
6	Komputer-6	19	XX	XX	XX	XX	XX
7	Komputer-7	7	XX	XX	XX	XX	XX

Gambar 14. Laporan Kesalahan Jaringan

V. KESIMPULAN

Berdasarkan hasil penelitian, maka dapat disimpulkan sebagai berikut :

1. Aplikasi *Network Management System* (NMS) yang dirancang dapat membantu seorang admin jaringan

dalam mengelola dan memelihara infrastruktur jaringan.

2. Perancangan dan implementasi sebuah aplikasi *Network Management System* (NMS) merupakan solusi yang efektif dalam mencari dan menemukan

kesalahan (*fault*) yang terdapat pada suatu jaringan. Efektif yang dimaksud di sini adalah dalam hal penyampaian kejadian *error* yang bersifat *real time* sehingga dapat dilakukan penanganan sedini mungkin agar masalah tersebut tidak berakibat pada penurunan kualitas jaringan.

3. Aplikasi *Network Management System* (NMS) yang dibangun dapat mengirimkan notifikasi kesalahan dan rekomendasi solusi melalui email kepada admin jaringan apabila terjadi kesalahan (*error*) pada jaringan.

DAFTAR PUSTAKA

- [1] Amar, F. L., 2015, Sistem Pemantauan Perangkat Jaringan Berbasis Web dengan Notifikasi Email dan Twitter, Skripsi Proyek Akhir Program Studi Diploma IV Teknologi Jaringan, Sekolah Vokasi, Universitas Gadjah Mada, Yogyakarta
- [2] Benu, D. O., Chandra, D. W., 2016, Penerapan *Fault Management* Menggunakan *Open Network Management System (OPENNMS)* Pada *Wireless Distribution System (WDS)*, Tugas Akhir Program Studi Teknik Informatika, Universitas Kristen Satya Wacana, Salatiga
- [3] Clemm, Alexander, 2007, *Network Management Fundamentals*, Cisco Press
- [4] Douglas R Mauro and Kevin J Schmidt, *Essential SNMP* 2nd Edition, 4th ed. United States of America: O'Reilly Media, 2011
- [5] Indarto, W., Zuhri, Z., Wijaya, S., 2015, Simple Network Management Protocol untuk Pemantauan Jaringan Dengan Pelaporan SMS, Seminar Nasional Aplikasi Teknologi Informasi 2015 (SNATI 2015)
- [6] MacIntyre, P., 2010, *PHP : The Good Parts Delivering the Best of PHP*, O'Reilly Media
- [7] Mutaqin, A. F., 2016, Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort, *Jurnal Sistem dan Teknologi Informasi (JUSTIN)* Vol. 1, No. 1, (2016)
- [8] Network Management System : Best Practices White Paper <http://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html> Updated July 11, 2007 diakses pada 11 Juli 2017
- [9] Nugroho, M., Affandi, A., Rahardjo, D., S., 2014, Rancang Bangun Aplikasi Monitoring Jaringan Menggunakan SNMP (*Simple Network Management Protocol*) dengan Sistem Peringatan Dini dan *Mapping* Jaringan, *Jurnal Teknik POMITS*, Vol. 3, No. 1
- [10] Provan, K. G., Kenis, P., 2008, Modes of Network Governance : Structure, Management, and Effectiveness, *J Public Adm Res Theory* (2008) 18 (2): 229-252, published on 02 August 2007
- [11] Reese, B., 2008, Top 25 Network Problems and Their Business Impact, Brad Reese on CISCO, *Network World*
- [12] Solehuddin, M., Sugiyono, Awaludin, M., 2016, Penerapan Simple Network Management Protocol Pada FCAPS untuk Monitoring Server Berbasis Android Studi Kasus PT. JARING SYNERGI MANDIRI, *Jurnal CKI On SPOT*, Vol. 9, No. 2, Desember 2016
- [13] Teoh, K. S., 2009, Email Services Server by Using the Simple Mail Transfer Protocol (SMTP), *Universiti Teknologi Malaysia*
- [14] Wijayanto, D., Waspada, I., 2016, Aplikasi Monitoring Perangkat dan Aktivitas Pengguna pada Jaringan menggunakan Protocol SNMP dan Squid Proxy, *Jurnal TEKNO SI*, Vol. 02, No. 03, Desember 2016